
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA : **CRIMINAL COMPLAINT**
 :
 v. : Honorable Cathy L. Waldor
 :
 ONUR AKSOY : Mag. No. 22-9260
 a/k/a "Ron Aksoy" :
 : **FILED UNDER SEAL**

I, Brent Rogan, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations, and that this complaint is based on the following facts:

SEE ATTACHMENT B

by phone

Brent Rogan, Special Agent
U.S. Department of Homeland Security
Homeland Security Investigations
*Special Agent Brent Rogan attested to this Affidavit by
telephone pursuant to FRCP 4.1(b)(2)(A).*

Sworn to before me telephonically
on June 29, 2022

Honorable Cathy L. Waldor
United States Magistrate Judge

s/Cathy L. Waldor 6/29/22
Signature of Judicial Officer

ATTACHMENT A**COUNTS 1-3**
(Mail Fraud)

From at least as early as in or about August 2013 through at least as recently as in or about April 2022, in the District of New Jersey and elsewhere, the defendant,

ONUR AKSOY
a/k/a "Ron Aksoy,"

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud victims of money and property, and on or about the dates listed below, in Monmouth County, in the District of New Jersey, and elsewhere, for the purpose of executing and attempting to execute this scheme and artifice to defraud, did knowingly cause to be delivered by private and commercial interstate carriers according to the direction thereon the shipments listed below, each shipment constituting a separate Count of this Complaint:

| Count | Approximate Date Shipment Received | City and State Shipment Received | Carrier | Contents of Shipment |
|--------------|---|---|----------------|---|
| 1 | February 2, 2018 | Red Bank, New Jersey | UPS | (1) counterfeit Cisco switch with part number WS-2960S-48FPD-L with counterfeit Cisco labels |
| 2 | February 2, 2018 | Red Bank, New Jersey | UPS | (1) counterfeit Cisco switch with part number WS-C2960X-48FPS-L with counterfeit Cisco labels |
| 3 | December 18, 2019 | Red Bank, New Jersey | UPS | (1) counterfeit Cisco switch with part number WS-C2960S-48FPD-L with counterfeit Cisco labels |

In violation of Title 18, United States Code, Section 1341.

ATTACHMENT B

I, Brent Rogan, am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Background

1. At times relevant to this Complaint:

a. The defendant, ONUR AKSOY, also known as “Ron Aksoy” (“AKSOY”), was a New Jersey resident from at least as early as in or about 2013 through in or about August 2016. AKSOY has been a Florida resident since in or about August 2016.

b. AKSOY created, owned, and controlled “Pro Network,” a criminal operation that purported to be in the business of selling genuine, high-quality computer networking equipment. AKSOY variously described himself as “President,” “CEO,” and “Founder” of Pro Network.

c. AKSOY operated Pro Network through a multitude of business entities and merchant and trade names under his full ownership and control.

d. Cisco Systems, Inc. (“Cisco”) was a multinational corporation headquartered in San Jose, California that designed, manufactured, and sold computer networking equipment.

Overview of the Scheme

2. An investigation conducted by HSI, General Services Administration-Office of Inspector General (“GSA-OIG”), the Defense Criminal Investigative Service (“DCIS”), the Naval Criminal Investigative Service (“NCIS”), and U.S. Customs and Border Protection (“CBP”) has shown that AKSOY has, from at least as early as in or about August 2013 through at least as recently as in or about April 2022, orchestrated a massive and fraudulent operation to traffic in counterfeit goods. During this period, AKSOY schemed with others to import from suppliers in China and Hong Kong counterfeit, low-quality computer networking devices made to appear like new and genuine devices manufactured by Cisco and to resell those devices in the United States and around the world, falsely representing those devices to buyers as new and genuine Cisco products.

During the scheme, AKSOY and his coconspirators imported and resold tens of thousands of counterfeit, low-quality Cisco devices, new and genuine versions of which carried a total retail value in the hundreds of millions of dollars.

3. Emails and other Pro Network business records obtained from this investigation show that beginning at least as early as in or about 2014, AKSOY would regularly purchase large quantities of counterfeit Cisco products from various illicit suppliers of counterfeit Cisco products based in China and Hong Kong (the “Counterfeit Suppliers”), causing those products to be shipped from China and Hong Kong to the United States. These products were typically accompanied by counterfeit Cisco labels, stickers, boxes, documentation, and/or packaging and were made to appear like new and genuine computer networking equipment manufactured and authorized by Cisco—even though they were not. The counterfeit Cisco products suffered from numerous and significant performance, functionality, and safety problems. At times, the counterfeit products would simply fail or otherwise malfunction, causing substantial damage to their users’ networks and operations and, in some cases, costing their users tens of thousands of dollars.

4. Emails and other Pro Network business records obtained from this investigation show that AKSOY and his subordinates at Pro Network would purchase counterfeit Cisco products from the Counterfeit Suppliers for as much as approximately 95 to 98 percent off of Cisco’s manufacturer’s suggested retail price (“MSRP”), far below the prices offered for genuine Cisco products by authorized Cisco resellers.

5. Investigation has revealed that AKSOY and the Counterfeit Suppliers would take a variety of measures to evade detection by CBP of the counterfeit Cisco products they were importing into the United States. For example, AKSOY and the Counterfeit Suppliers would routinely break up large orders of counterfeit Cisco products into multiple smaller shipments dispatched on different days and ship counterfeit Cisco products to undeliverable addresses, changing those shipments’ final shipping addresses to Pro Network’s headquarters only after they had cleared inspection by CBP.

6. Bank records reviewed by law enforcement show that AKSOY would wire payment for the counterfeit Cisco products to the Counterfeit Suppliers’ overseas bank accounts from U.S. bank accounts under his ownership and control. In all, AKSOY wired at least approximately \$55 million to Counterfeit Supplier bank accounts.

7. AKSOY and his Pro Network subordinates would then sell these counterfeit Cisco products through a variety of channels, including Amazon, eBay, and direct sales. AKSOY and his Pro Network subordinates and co-schemers would falsely represent these counterfeit Cisco products on these channels as genuine, new, and factory-sealed Cisco products. End users of these

counterfeit devices included hospitals, schools, government agencies, and the military.

8. Based on, among other things, bank and Pro Network business records reviewed by law enforcement, in all, AKSOY generated at least approximately \$100 million in gross revenue through the sale of counterfeit Cisco products during the scheme.

9. AKSOY received frequent notifications throughout the scheme that the purported Cisco products he was purchasing and reselling were counterfeits. For example:

a. Between in or about February 2014 and in or about April 2022, CBP officials seized approximately 180 shipments of counterfeit Cisco products, comprising approximately 860 counterfeit devices, from numerous Counterfeit Suppliers to AKSOY and various Pro Network entities. The total MSRP of genuine versions of these seized counterfeit Cisco products exceeded \$5 million.

b. Between in or about June 2014 and in or about August 2019, Cisco sent at least seven cease-and-desist letters to AKSOY and various Pro Network entities demanding that they stop trafficking in counterfeit Cisco products.

c. Emails, business records, and other evidence reviewed by law enforcement show that AKSOY also received numerous complaints from Pro Network's customers, in some cases from end users who purchased directly from Pro Network entities and in other cases from resellers who purchased from Pro Network entities, often passing on complaints they had received from the end users. Customers and resellers complained that the devices they had obtained from Pro Network were counterfeit, substandard, used, or broken; had missing parts; did not work; were either not covered or were not eligible for Cisco technical support coverage; and in some instances had caused significant damage to these customers' networks and operations.

d. Amazon routinely terminated specific product listings for purported Cisco products on Amazon storefronts under the control of AKSOY and Pro Network, and even entire storefronts, in response to counterfeit complaints from customers and Cisco.

10. Despite these and other notifications, AKSOY continued purchasing and reselling counterfeit Cisco products from the same Counterfeit Suppliers throughout the scheme.

The July 2021 Search

11. During the execution of a search warrant at Pro Network's warehouse and headquarters in Doral, Florida on or about July 21, 2021, law enforcement discovered and seized approximately 1,156 purported Cisco devices that were determined through subsequent analysis to be counterfeit Cisco products. The total MSRP of these seized counterfeit Cisco products was approximately \$7,011,296.

The Charged Counterfeit Products

12. On or about the following dates, undercover members of law enforcement purchased and received shipment of the following purported Cisco products from Pro Network. Pro Network represented that each of these purported Cisco products was a new and genuine Cisco computer networking device but they were later found, upon further analysis, (i) to be a counterfeit Cisco product and (ii) to be accompanied by counterfeit Cisco labels, stickers, boxes, documentation, and/or packaging intended to make the counterfeit device appear like a new and genuine Cisco device.

| Count | Approximate Date Shipment Received | City and State Shipment Received | Carrier | Contents of Shipment |
|--------------|---|---|----------------|---|
| 1 | February 2, 2018 | Red Bank, New Jersey | UPS | (1) counterfeit Cisco switch with part number WS-2960S-48FPD-L with counterfeit Cisco labels |
| 2 | February 2, 2018 | Red Bank, New Jersey | UPS | (1) counterfeit Cisco switch with part number WS-C2960X-48FPS-L with counterfeit Cisco labels |
| 3 | December 18, 2019 | Red Bank, New Jersey | UPS | (1) counterfeit Cisco switch with part number WS-C2960S-48FPD-L with counterfeit Cisco labels |